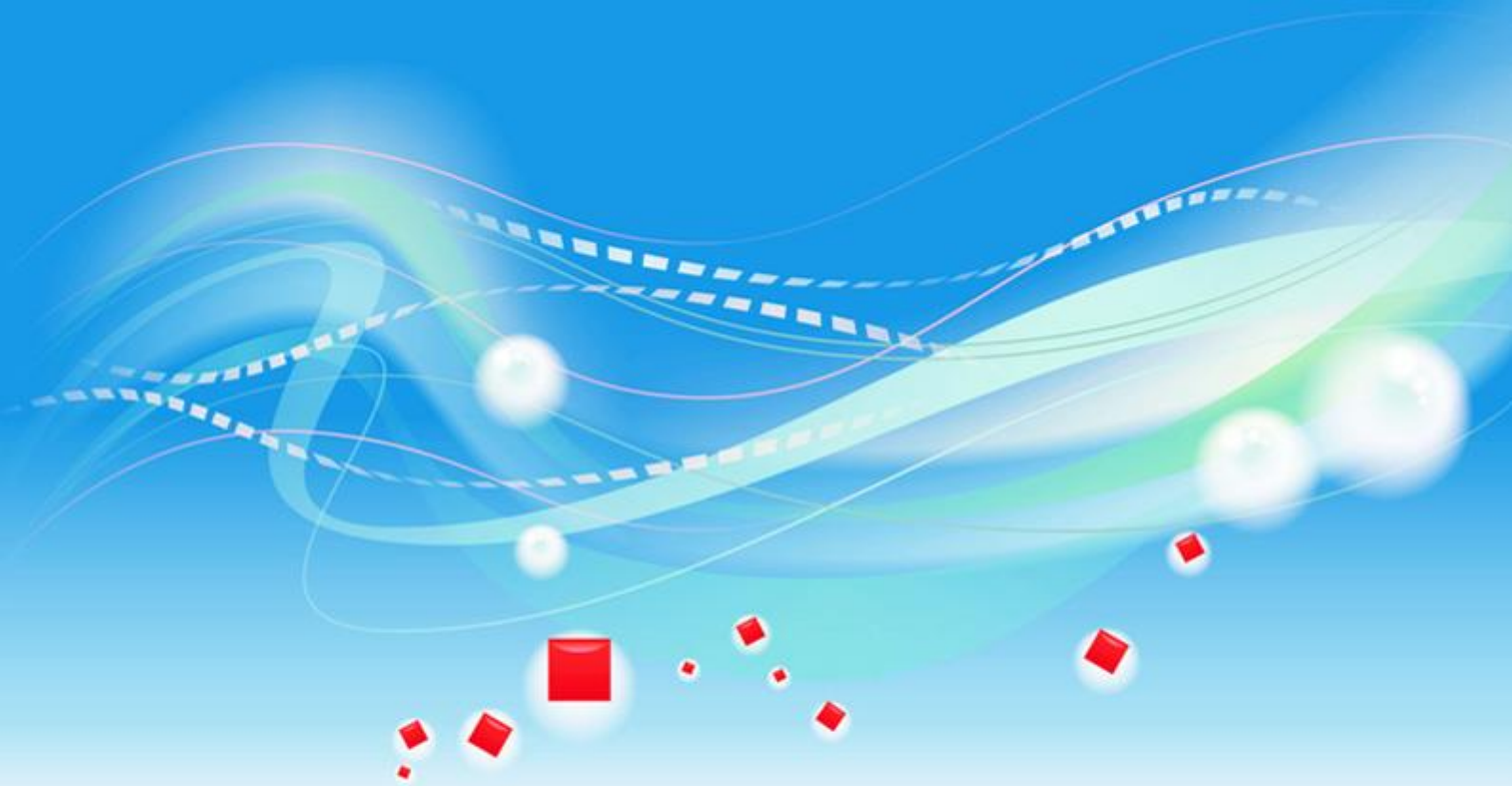


ViPNet Application Control 4.2

User's Guide

ViPNet Virtual Private Network

infotecs

© 1991–2013 Infotecs ®. All rights reserved.

Version: 00116-03 34 04 ENU

This document is included in the software distribution kit and is subject to the same terms and conditions as the software itself.

No part of this publication may be reproduced, published, stored in an electronic database, or transmitted, in any form or by any means — electronic, mechanical, recording, or otherwise — for any purpose, without the prior written consent of Infotecs JSC.

ViPNet is a registered trademark of Infotecs JSC, Moscow, Russia.

All brands and product names that are trademarks or registered trademarks are the property of their owners.

Infotecs GmbH

Oberwallstr. 24

10117 Berlin

Deutschland

Tel: +49 (0) 30 206 43 66 0

Fax: +49 (0) 30 206 43 66 66

Email: support@infotecs.biz

Web: http://www.infotecs.biz

Contents

Introduction **5**
About This Document 6
Audience 6
Document Conventions 6
About ViPNet Application Control 8
Application Control Purpose 8
System Requirements 8
Feedback 10

Chapter 1. General Information **11**
How Application Control Works 12
User Permissions for Application Control 13
Application Control Interface 14
Work with Application Control in a Terminal Session 16

Chapter 2. Quick Start **18**
How to Allow Network Activity for an Application 19
How to Block Network Activity for an Application 21
How to Disable Network Activity Requests 22
Registering an Application Without a Request 24

Chapter 3. Network Activity Tracking **25**
Starting and Exiting Application Control 26
How to Disable Application Control Automatic Start at Windows Startup 27
Configuring Network Access for an Application 28
Allow and Prompt a User Rule 29
Prompt the User Rule 29
Block and Prompt a User Rule 30
Configuring Network Service Access When You Work On a Terminal Server 31
Working with the Registered Applications List 33
Viewing the Registered Applications List 33
Changing Network Access Rules for an Application 35

Unregistering an Application 36
Disabling Network Activity Tracking 38
Changing a User 39
Changing a User When You Work in a Terminal Session 39
Logging onto Application Control as an Administrator 41
Logging onto Application Control As an Administrator When You Work in a Terminal Session 41

Chapter 4. Viewing Statistics and the Event Log 42
Viewing Statistics 43
Viewing the Event Log 44

Chapter 5. Configuring Application Control 46
Network Activity Tracking Options 47
Modifications Tracking Options 48
Processing Applications Network Access Requests in the Non-Interactive Mode 50
Event Log Options 52
Events Filter Options 54

Appendix A. Glossary 57

Appendix B. Index 60

Introduction

About This Document 6

About ViPNet Application Control 8

Feedback 10

About This Document

This document describes the purpose and scope of ViPNet Application Control, and its specifications. It contains all the information necessary to work with the program and configure it.

Audience

This document is intended for the users of the ViPNet software containing the ViPNet Application Control program.

To use this document efficiently, you should have basic knowledge of networks.

Document Conventions

This document concerns the following conventions:

Table 1: Document conventions

Icon	Description
	Warning: Indicates an obligatory action or information which may be critical for continuing user operations.
	Note: Indicates a non-obligatory, but desirable action or information which may be helpful for users.
	Tip: Contains additional information.

Table 2: Conventions for highlighted information

Icon	Description
Name	The name of an interface element. For instance, the name of a window, a box, a button or a key.
Key+Key	Shortcut keys. To use the shortcut keys, press and hold the first key and press other keys.
Menu > Submenu > Command	A hierarchical sequence of elements. For instance, menu items or sections in the navigation pane.
`Code`	A file name, path, text file (code) fragment or a command executed from the command line.

About ViPNet Application Control

Application Control Purpose

ViPNet Application Control provides constant tracking of network activity of the applications running on your ViPNet host. When an application displays network activity (for example, listens to a network port or sends packets to a network), it is registered in Application Control. You choose whether network access should be blocked or allowed for this application. Application Control protects your computer from many threats such as unauthorized access to user data or running spyware on it.

Application Control is the component of the ViPNet Client and ViPNet Coordinator software if it is allowed by the license file.

Note: In ViPNet VPN, Application Control is included only in ViPNet Coordinator.

System Requirements

You can't install ViPNet Application Control independently from the ViPNet software. That is why the system requirements for Application Control are defined by the system requirements for the ViPNet software it is a component of.

Table 3: Minimum system requirements for ViPNet software

System requirements	ViPNet Coordinator	ViPNet Client
Operating system	Microsoft Windows XP (32/64 bit), Server 2003 (32/64 bit), Vista (32/64 bit), Server 2008 (32/64 bit), Windows 7 (32/64 bit), Server 2008 R2 (64 bit), Windows 7 (32/64 bit), Windows 8 (32/64 bit), Server 2012 (64 bit).	
	Note: You must install the latest service pack for your version of Windows.	
Applications	Internet Explorer (if used) — version 6.0 and later.	
	No other program firewalls should be enabled.	
Processor	Pentium IV. We recommend Intel Core 2 Duo E6400 or another x86-compatible multicore processor of the same performance.	
RAM	1024 MB minimum.	512 MB minimum.
Disk space	300 MB minimum if you work with ViPNet Registration Point.	150 MB minimum.
	1000 MB minimum if you work with ViPNet Coordinator.	
Network interfaces	Any that support IPv4.	Any that support IPv4.

Feedback

Finding Additional Information

For more information about Infotecs products and technologies, see the following resources:

- ViPNet documentation web portal http://www.infotecs.biz/doc_vipnet/ENU/index.htm.
- Information about current Infotecs products http://infotecs.biz/products/.
- Information about Infotecs solutions http://infotecs.biz/solutions/.
- Frequently asked questions http://www.infotecs.biz/doc_vipnet/ENU/index.htm#3_17014.htm.

Contacting Infotecs

We value any feedback from you. If you have any questions concerning Infotecs products and solutions, any suggestions, complains or other feedback, feel free to contact us by means of the following:

- Support request form http://infotecs.biz/support/.
- Support email: support@infotecs.biz.
- Telephone: +49 (0) 30 206 43 66 0.
- Fax: +49 (0) 30 206 43 66 66.

Errata

Infotecs makes every effort to ensure that there are no errors or misprints in the text of all documents supplied with ViPNet software. However, no one is perfect, and mistakes do occur. If you find an error in one of our documents, like a spelling mistake or some inaccuracy in describing user scenarios or system features, we would be very grateful for your feedback. By sending in errata you may save other reader hours of frustration, and at the same time you will be helping us provide documentation in even higher quality.

1

General Information

How Application Control Works 12

User Permissions for Application Control 13

Application Control Interface 14

Work with Application Control in a Terminal Session 16

How Application Control Works

ViPNet Application Control tracks the following network activities of applications running on a ViPNet host:

- attempts to access the network;
- attempts to open ports for inbound connections;
- sends packets without establishing connection.

In case Application Control detects network activity of an application, you are prompted to block or allow access to the network for this application. For the program to allow or block access automatically, configure network access rules for this application. Also you can configure the non-interactive mode for this application (see Non-interactive mode on page 57).

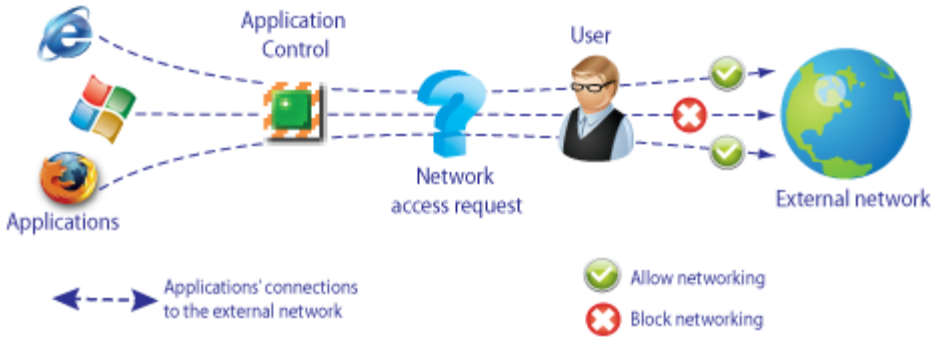


Figure 1: Application Control operation principle

As soon as you explicitly allow or block access to the network for an application, Application Control registers the application. This means that Application Control will remember the action you choose for the application and apply it automatically at the next network activity of the application.

User Permissions for Application Control

In ViPNet CUSTOM, depending on the user permissions level (see User permissions on page 58) specified for your ViPNet host, you can or can't change some Application Control settings. The ViPNet network administrator defines permissions levels in ViPNet Administrator. For more information about user permissions, see "ViPNet User Permissions. Supplement to ViPNet documentation."

When you work with ViPNet VPN, full Application Control functionality is available.

Note: If you need to configure some options unavailable to you, contact your ViPNet network administrator (on page 58). For information on how to log on as a ViPNet host administrator (see Logging onto Application Control as an Administrator on page 41).

If you work in a ViPNet CUSTOM network on a host with ViPNet Client or ViPNet Coordinator software installed and:

- the maximum permission level is specified for your ViPNet host (on page 58), full Application Control functionality will be available to you.
- the minimum or average permission level is specified for your ViPNet host, the program functionality will be restricted in the following way:
  - The **Settings** section is unavailable.
  - In the **Log Settings** subsection of the **Event Log** section, only the options under **Show event log** are available.
  - You can't edit the lists of allowed and blocked applications.
  - You can't disable ViPNet Application Control (on the **Service** menu, the **Disable Tracking** and **Exit** menu items are unavailable).

For more information about special permission levels, see "ViPNet User Permissions. Supplement to ViPNet documentation."

Note: If you accept a keys update limiting user permissions, Application Control functionality will be restricted only after Application Control restart.

Application Control Interface

The main ViPNet Application Control window is shown in the figure below:

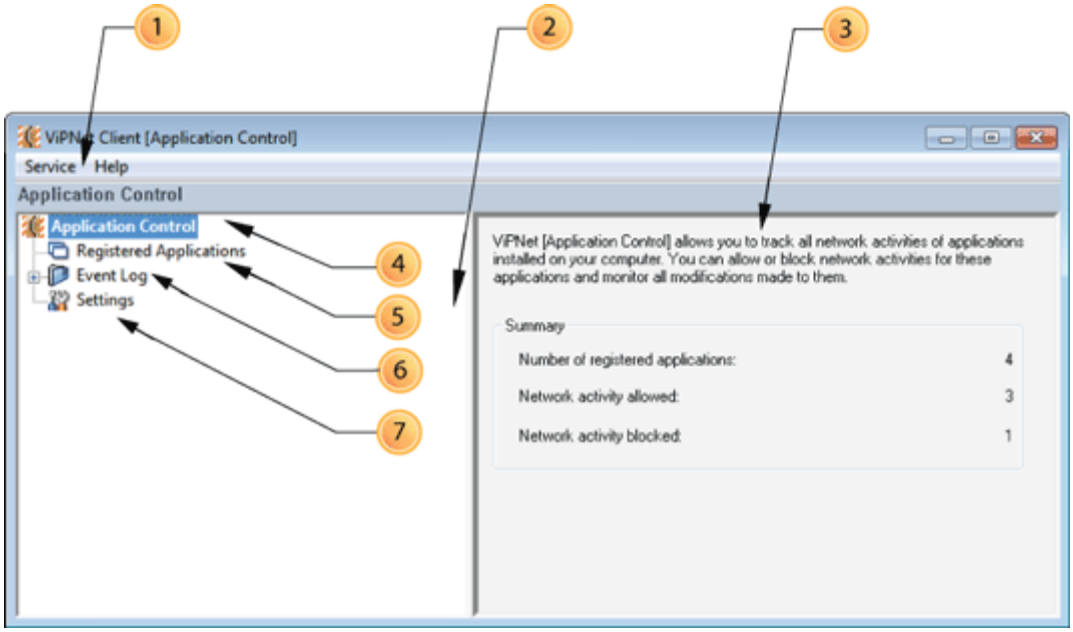


Figure 2: ViPNet Application Control main window

The following interface elements are numerated:

1 The menu bar.

2 The navigation pane, where the main program features are displayed as sections.

3 The view pane, where the contents of the section selected in the left pane are displayed.

4 The **Application Control** section. Select this element to view information about the program purpose (see About ViPNet Application Control on page 8) and statistics (see Viewing Statistics on page 43)about applications whose network activity has been allowed or blocked.

5 The **Registered Applications** section. Select this element to view information about the applications registered in Application Control.

In the **Registered Applications** section, you can change the network access rules (see Changing Network Access Rules for an Application on page 35) for a registered application or unregister an application (see Unregistering an Application on page 36).

6 The **Event Log** section. Select this element to view information about changes in network access rules for an application. Select **Log Settings** to set the log options (see Event Log Options on page 52). Select Filter Settings to set a filter for displaying events in the log (see Events Filter Options on page 54).

7 The **Settings** section. Select this element to configure network activity tracking (see Network Activity Tracking Options on page 47) and modifications in applications (see Modifications Tracking Options on page 48).

Work with Application Control in a Terminal Session

When Application Control is running on a terminal server, every user can allow or block network access of applications running in this user's session, allow or block network services activity, and change program options for all user sessions if he or she has sufficient permissions (see User Permissions for Application Control on page 13). Work with Application Control on a terminal server has some peculiarities.

If several user sessions are active on a terminal server and one of the users configures Application Control (see Configuring Application Control on page 46), the changes will be applied in all the user sessions, and Application Control graphical interface will be updated in all user sessions according to the new options.

If several users configure Application Control at once, only the changes made by the user who saves them first will be applied. Other users will be notified that the program options have been changed by another user when they try to save their changes.

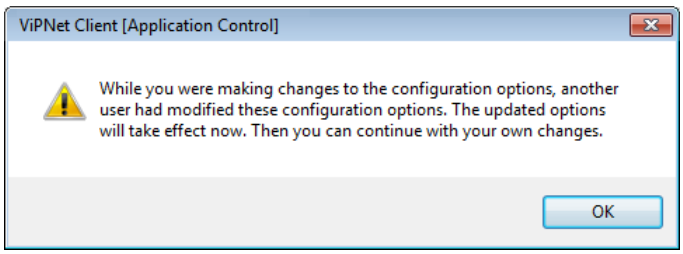

ViPNet Client [Application Control]
While you were making changes to the configuration options, another user had modified these configuration options. The updated options will take effect now. Then you can continue with your own changes.
OK

Figure 3: Notification that Application Control options have already been changed by another user

If one of the users runs an application trying to access network, the request window will be displayed only to this user.

If an application has been registered in one of the user sessions, it will be displayed as a registered application (see Viewing the Registered Applications List on page 33) in all user sessions. For details, see Configuring Network Service Access When You Work On a Terminal Server (on page 31).

For the information about logging onto Application Control as another user or as an administrator when you work in a terminal session, see:

- Changing a User When You Work In a Terminal Session (on page 39);

- Logging Onto Application Control As an Administrator When You Work In a Terminal Session (on page 41).

Let's explain how an application is registered when Application Control is running on a terminal server:

1. On the terminal server, the ViPNet software with the Application Control program is installed, and the following conditions are met:
   - the average permissions level (see User Permissions for Application Control on page 13) is set for the host;
   - User A is the ViPNet host administrator (see ViPNet host administrator's password on page 58);
   - in the **Settings** section, the **Start automatically upon ViPNet authentication on Windows logon** check box is selected;
   - the **Prompt the user** network access rule (see Prompt the User Rule on page 29) has been chosen.
2. User B logs onto the terminal server with his or her Windows user account for remote work.
3. In User B's session, Application Control starts automatically.
4. User B starts Internet Explorer and is notified that Internet Explorer has tried to access the network. In the request window, the user is prompted to choose an action for Application Control to apply to Internet Explorer.
5. User B allows the application to access the network.
6. The application is registered in Application Control as one allowed to access the network. The registered applications list (see Working with the Registered Applications List on page 33) is refreshed in both users' sessions.

If User B decides later that Internet Explorer network activity should be blocked or Internet Explorer should be unregistered, this user will not be able to do that, as the average permission level is not sufficient for making those settings. In this case, User B should contact User A and ask him or her to log onto Application Control as the ViPNet host administrator (see Logging onto Application Control As an Administrator When You Work in a Terminal Session on page 41) and configure the required options.

If a service on a terminal server (see Configuring Network Service Access When You Work On a Terminal Server on page 31) tries to access the network, Application Control work mechanism will be different.

2

Quick Start

How to Allow Network Activity for an Application 19

How to Block Network Activity for an Application 21

How to Disable Network Activity Requests 22

Registering an Application Without a Request 24

How to Allow Network Activity for an Application

As soon as you install ViPNet Application Control, it starts tracking network activity of applications running on your computer. By default, all applications are allowed to access the network. That is why, once an application becomes active in the network, a message, informing you that it attempted to access network and was allowed to do that, will be displayed. In the message window, select the action you want Application Control to apply to this application at its next network activity (that is, set a network activity mode for the application).

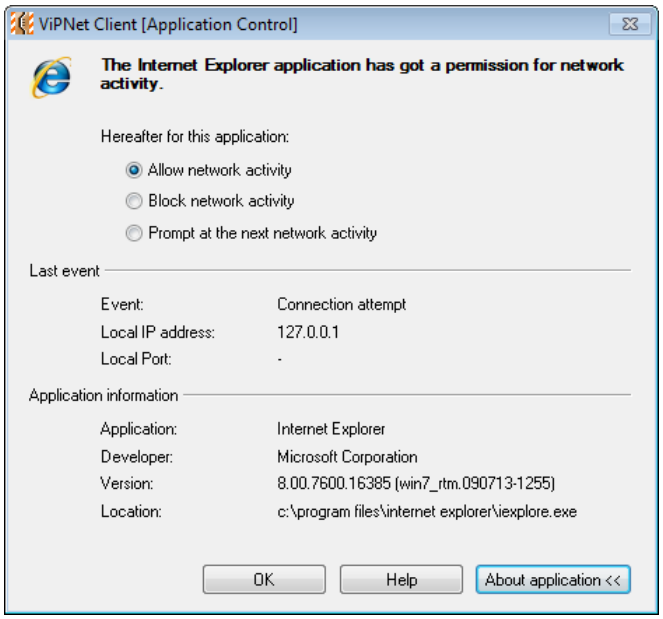


Figure 4: Network access request window

To allow application network activity:

1. In the request window, select **Allow network activity**.
2. Click **OK**.

As a result, network activity of the application will be allowed.

If you need to allow application network activity at the next connection attempt, but you want to see the request window again to be able to choose further network activity mode for the application:

1. In the request window, select **Prompt at the next network activity**.
2. Click **OK**.

As a result, next time the application will be allowed to access the network and the request window, informing you that the program attempted and was allowed to access the network, will be displayed once more.

How to Block Network Activity for an Application

Once Application Control detects network activity of an application, the request window, informing you that this application attempted to access the network and was allowed to do that, will be displayed. In the request window, you can immediately block network activity for the application:

1. In the request window, select **Block network activity**.
2. Click **OK**.

As a result, this application will not be able to connect to the network.

To allow network activity for a blocked application, either:

- delete the application from the list of registered applications (see Unregistering an Application on page 36) and re-register it, or
- change the network activity mode (see Changing Network Access Rules for an Application on page 35) for the application.

How to Disable Network Activity Requests

If you do not want ViPNet Application Control to request you about allowing or blocking network activity for an application:

1. In the main Application Control window, in the navigation pane, select **Settings**.
2. In the **Settings** section, under **Application control rules**, in the **At application network activity** list, select one of the following:
   - **Allow network activity** if you want unregistered applications to connect to the network.
   - **Block network activity** if you do not want unregistered applications to connect to the network.

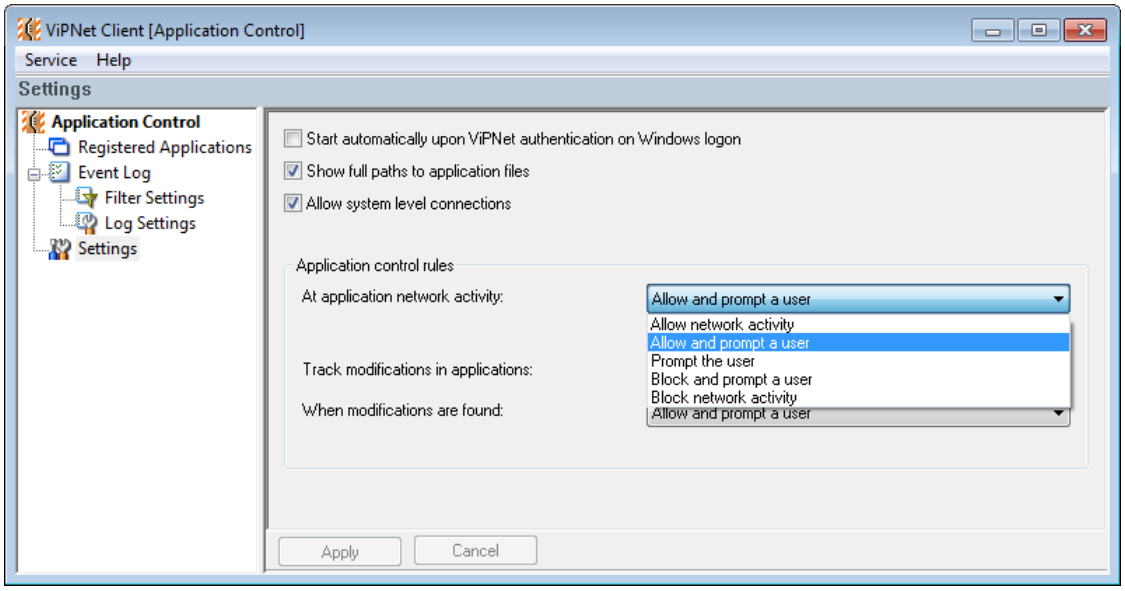


Figure 5: Defining a single network access policy for applications

3. Click **Apply**.

As a result, the chosen network activity rule will be applied to unregistered applications automatically.

To disable notifications in Application Control, you can also disable network activity tracking (see Disabling Network Activity Tracking on page 38).

Registering an Application Without a Request

Any application, that has not displayed network activity yet, or for which you have previously selected **Prompt at the next network activity, Allow once** or **Block once**, is considered "unregistered". If you need to configure network activity rules for such an application, you should register it. To do that:

1. On the **Service** menu, select **Register application**.
2. Then, click **With Network Activity Allowed** (to allow your program to access the network) or **With Network Activity Blocked** (to prevent your program from connecting to the network).
3. In the **Add Program to the Registered Applications List** window, navigate to the executable file (`*.exe`) of the application you want to allow or block, select it and click **Open**.

As a result, in the **Registered Applications** section, you can view the selected application with the **Allowed** or **Blocked** status displayed in the **Network Activity** column.

Thus, the selected application will be registered in ViPNet Application Control, and network activity will be either allowed or blocked for it.

3

Network Activity Tracking

Starting and Exiting Application Control	26
How to Disable Application Control Automatic Start at Windows Startup	27
Configuring Network Access for an Application	28
Working with the Registered Applications List	33
Disabling Network Activity Tracking	38
Changing a User	39
Logging onto Application Control as an Administrator	41

Starting and Exiting Application Control

In ViPNet CUSTOM, ViPNet Application Control automatically starts together with the ViPNet software as its component. When necessary, you can cancel the program automatic startup (see How to Disable Application Control Automatic Start at Windows Startup on page 27).

In ViPNet VPN, the first start of Application Control can be performed only manually. If necessary, further you can configure automatic start.

To start the Application Control program manually, in the main window of the ViPNet Client or ViPNet Coordinator program, in the **Applications** menu, select **Application control**.

To exit Application Control, do one of the following:

- In the top-right corner of the main window, click **Close** .
- Press **Alt+F4**.

As a result, network activity tracking will be disabled.

For information about disabling network activity tracking, see Disabling Network Activity Tracking (on page 38).

How to Disable Application Control Automatic Start at Windows Startup

For ViPNet Application Control not to start automatically as you log onto the ViPNet software at Windows startup:

1 In the main window, in the navigation pane, select **Settings**.

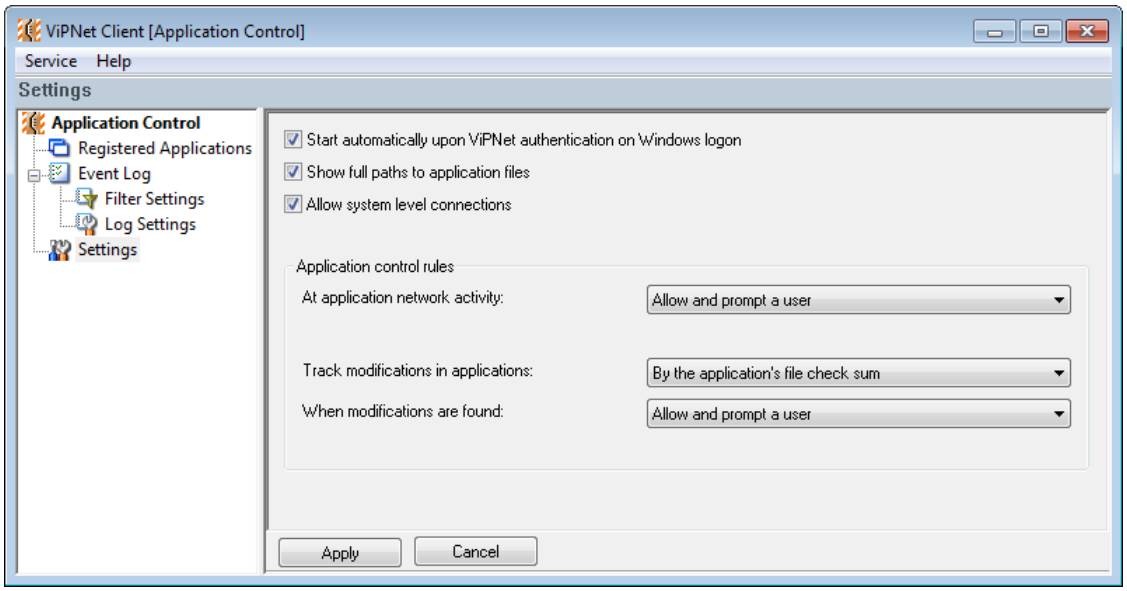


Figure 6: Application Control program options

2 In the **Settings** section, clear the **Start automatically upon ViPNet authentication on Windows logon** check box.

3 Click **Apply**.

As a result, Application Control will not start automatically as you log onto the ViPNet software at Windows startup. To enable network activity tracking, you should start Application Control manually (see Starting and Exiting Application Control on page 26).

You can't start Application Control when the ViPNet software, it is a component of, is not running. That is why, if you cancel starting the ViPNet software at Windows startup, Application Control will not be launched either. If, after Windows startup, you start the ViPNet software manually, you should start Application Control manually as well (see Starting and Exiting Application Control on page 26).

Configuring Network Access for an Application

The main purpose of ViPNet Application Control is to track network activity of applications running on your computer and register these applications. You are prompted to choose whether you allow network activity for an application in the following cases:

- The application is not registered in Application Control.
- The application has been deleted from the list of registered applications (see Unregistering an Application on page 36).
- The application had been registered in Application Control, but its parameters were modified (see Modifications Tracking Options on page 48), for example, the application was updated to a later version.

Once network activity of an application is detected, this application is allowed to access the network, and you are prompted to define a network activity rule for it. At the next connection attempt, ViPNet Application Control will apply the corresponding action to this application.

The request window displayed depends on the network activity rule (see Network Activity Tracking Options on page 47) defined for this application previously. In Application Control, you can define one of the following network activity rules for an application:

- Allow network activity.
- Allow and prompt a user.
- Prompt the user.
- Block and prompt a user.
- Block network activity.

If you choose **Allow network activity** or **Block network activity**, the corresponding rule will be further applied without prompting.

Allow and Prompt a User Rule

If the default network activity rule (**Allow and prompt a user**) is set for an application, the application is allowed to connect to the network, but you are prompted to define the action to be applied to this application next time. In the non-interactive mode (on page 57), network activity will be allowed for the application.

If the **Allow and prompt a user** rule is set for an application, to allow the application to establish connection to the network, complete the steps described in How to Allow Network Activity for an Application (on page 19).

If the **Allow and prompt a user** rule is set for an application, to block access to the network for the application, complete the steps described in How to Block Network Activity for an Application (on page 21).

Prompt the User Rule

If, in the **Application Control** section, you choose the **Prompt the user** network access rule (see Network Activity Tracking Options on page 47), no rule will be applied to the application at its next connection attempt, until you explicitly specify whether you allow or block connection.

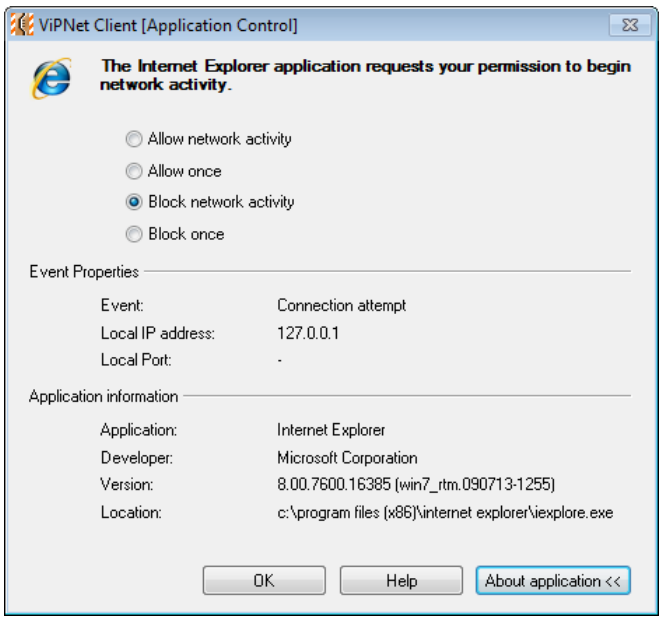


Figure 7: The request window when the "Prompt the user" policy is set

Tip: To show or hide information about an application, in the request window, use the **About application** button.

If the **Prompt the user** rule is set for an application, to allow the application to connect to the network:

1. In the request window, select either:
   - **Allow network activity**, and the application will be registered and allowed to connect to the network, or
   - **Allow once**, and in the current session, the application will be allowed to connect to the network. At the next network activity of the application, you will be prompted to allow or block access to the network again.
2. Click **OK**.

If the **Prompt the user** rule is set for an application, to block network activity for the application:

1. In the request window, select either:
   - **Block network activity**, and the application will be registered, while any network activity of the application will be blocked.
   - **Block once**, and in the current session, any network activity of the application will be blocked. At the next network activity of the application, you will be prompted to allow or block access to the network again.
2. Click **OK**.

If the **Prompt the user** network access activity is set and an application tries to access the network, but you can't choose an action in the request window at the moment, Application Control will process applications network access requests in the non-interactive mode (on page 57). For details, see Processing Applications Network Access Requests in the Non-Interactive Mode (on page 50).

Block and Prompt a User Rule

If the **Block and prompt a user** rule is set, applications are not allowed to access the network, and you are prompted to define the action to be applied to this application at its next network activity. In the non-interactive mode, network activity will be blocked for the application.

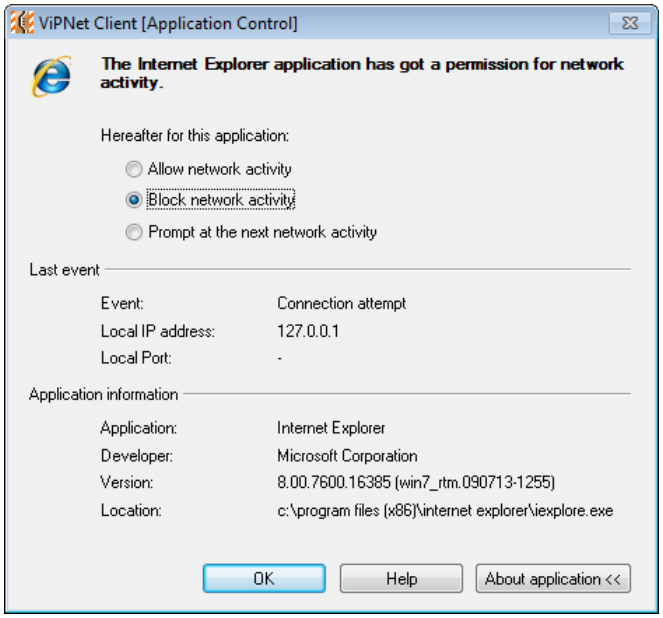


Figure 8: The request window when the "Block and prompt a user" policy is set

If the **Block and prompt a user** rule is set for an application, to allow the application to connect to the network:

1. In the request window, select either:
   - **Allow network activity**, to allow the application to connect to the network, or
   - **Prompt the user**, to allow the application to connect to the network only in the current session. At the next network activity of the application, you will be prompted whether to allow or block connection again.
2. Click **OK**.

If the **Block and prompt a user** rule is set for an application, to block network access for the application:

1. In the request window, select **Block network activity** (the request window will not be displayed at the next application network activity).
2. Click **OK**.

Configuring Network Service Access When You Work On a Terminal Server

If a network service on a terminal server tries to access the network, a user working on this server will be notified about it and prompted to define the action Application Control should

apply to the service. Only one user can be notified. If there are several active user sessions on the terminal server, the notification will be displayed in a user session according to the following priority-based order:

1. a local user authorized as the ViPNet host administrator;
2. a remote user authorized as the ViPNet host administrator;
3. a local user authorized as a ViPNet host user;
4. a remote user authorized as a ViPNet host user.

For example:

1. On a terminal server, two user sessions are running:
   - User A is a local user authorized as a ViPNet host user;
   - User B is a remote user authorized as the ViPNet host administrator.
2. On the terminal server, the BranchCache network service tries to access the network.
3. User B will be notified about it and will choose one of the actions in the request window.
4. Application Control will apply the chosen action to the network service.
5. If the service will be registered as one allowed or prohibited to access the network (see Quick Start on page 18), it will be displayed in the registered applications list in both users' sessions.

Working with the Registered Applications List

Viewing the Registered Applications List

In ViPNet Application Control, you can view information about the applications registered, whose network access has been allowed or blocked. To do this, in the navigation pane of the main Application Control window, select **Registered Applications**.

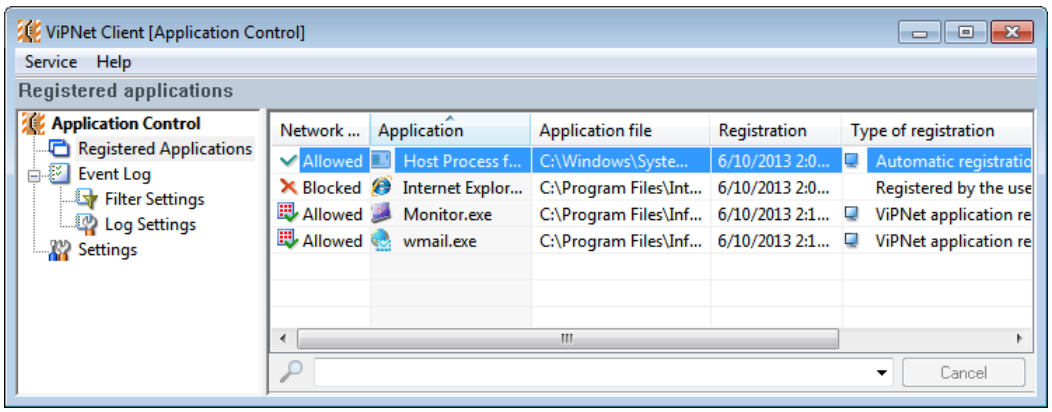


Figure 9: Viewing the parameters of registered applications

As a result, in the view pane, the following information about the registered applications will be displayed in a table-like list:

1. In the **Network activity** column, you can see whether network access is allowed or blocked for the application. The following modes of network activity are possible:
   - **Allowed** if the application's network activity is allowed.
   - **Blocked** if the application's network activity is not allowed.
   - **Allowed** if the ViPNet application's network activity is allowed.
   - **Blocked** if the ViPNet application's network activity is not allowed.
2. In the **Application** column, you can see registered applications names.
3. In the **Application file** column, by default, the path to the executable file of the registered application is displayed. If you want only the executable file to be displayed:

- In the navigation pane, select **Settings**.
- In the view pane, clear the **Show full paths to application files** check box.

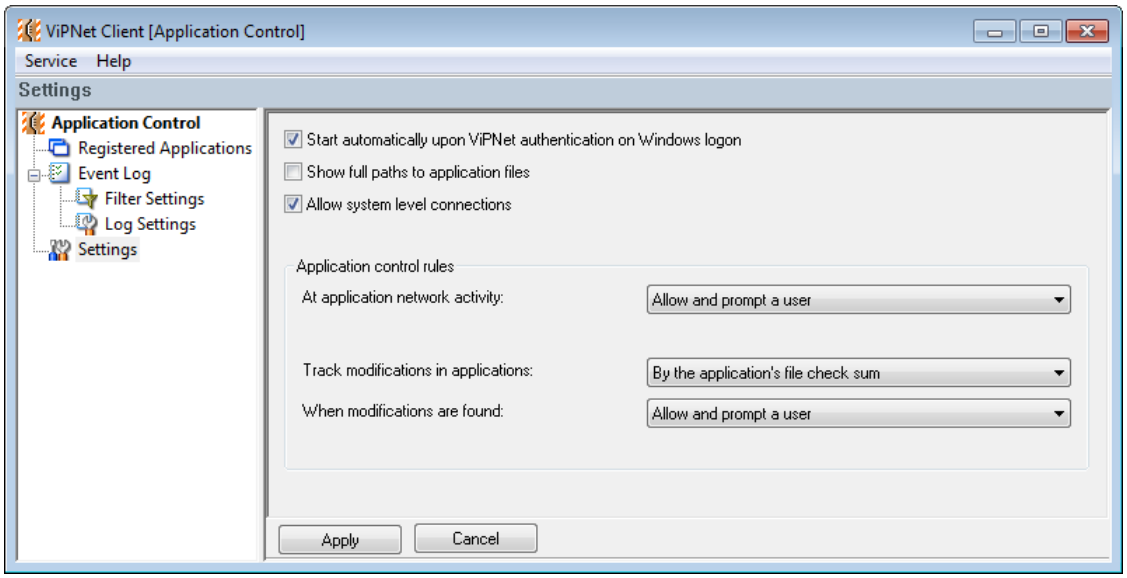


Figure 10: Choosing the way the executable file name and path will be displayed

4 In the **Registration** column, start date and time of network activity monitoring are displayed.

5 In the **Type of registration** column, one of the following application registration types is displayed:

- **Registered by the user**, if you chose **Prompt the user** (see Prompt the User Rule on page 29) while configuring a network access mode or registered the application manually (see Registering an Application Without a Request on page 24).
- **Automatic registration,** if you chose any option but **Prompt the user** while configuring a network access mode (see Configuring Network Access for an Application on page 28).
- **ViPNet application registration**, if the application registered is one of ViPNet applications.
- **Application modification by user request,** if you chose Prompt the user while configuring monitoring of registered applications modifications (see Modifications Tracking Options on page 48).
- **Automatic registration when application is modified**, if you chose any option but Prompt the user while configuring monitoring of registered applications modifications (see Modifications Tracking Options on page 48).
- **ViPNet application update**, if Application Control tracked a modification in a registered ViPNet application.

6 In the **Application modification** column, the last application modification date and time are displayed (see Modifications Tracking Options on page 48). If this application has not been modified, the corresponding entry will be empty.

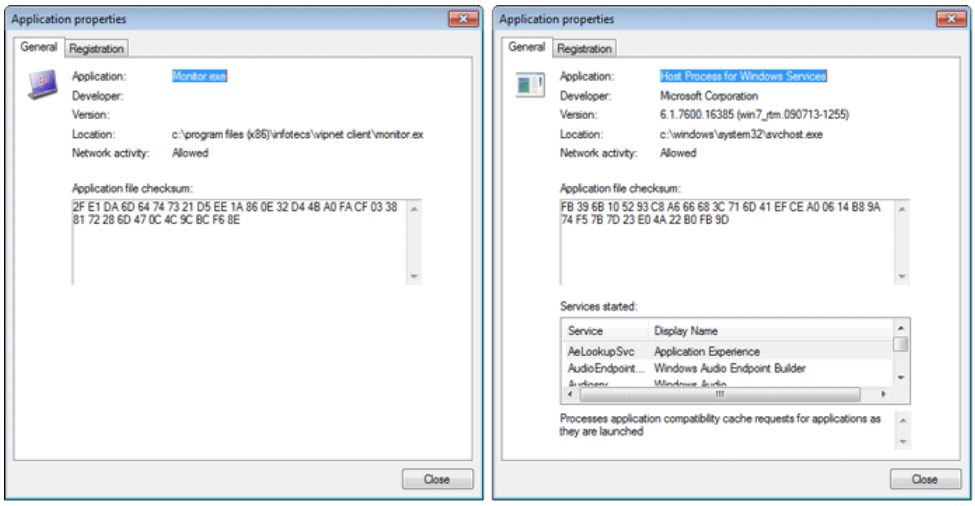
To change the details displayed in the **Registered applications** section, right-click any column header and select or clear the corresponding check boxes.

To view registered application properties in a separate window:

1 In the **Registered applications** section, right-click the entry corresponding to the application to view properties of.

2 Click **Application Properties**.

As a result, the application properties and registration data will be displayed in a separate window. In the **Application properties** dialog box of a host process, you can also see a list of services working in the process and some general information about them.



ViPNet Monitor application properties **Svchost.exe host process properties**

Figure 11: Viewing application properties

Changing Network Access Rules for an Application

To change network access rules for a registered application (that is, an application for which **Allow network activity** or **Block network activity** action has been selected in the request window):

1 In the main Application Control window (see Application Control Interface on page 14), in the navigation pane, select **Registered applications**.

2 In the view pane, right-click the entry corresponding to the application whose options you need to change.

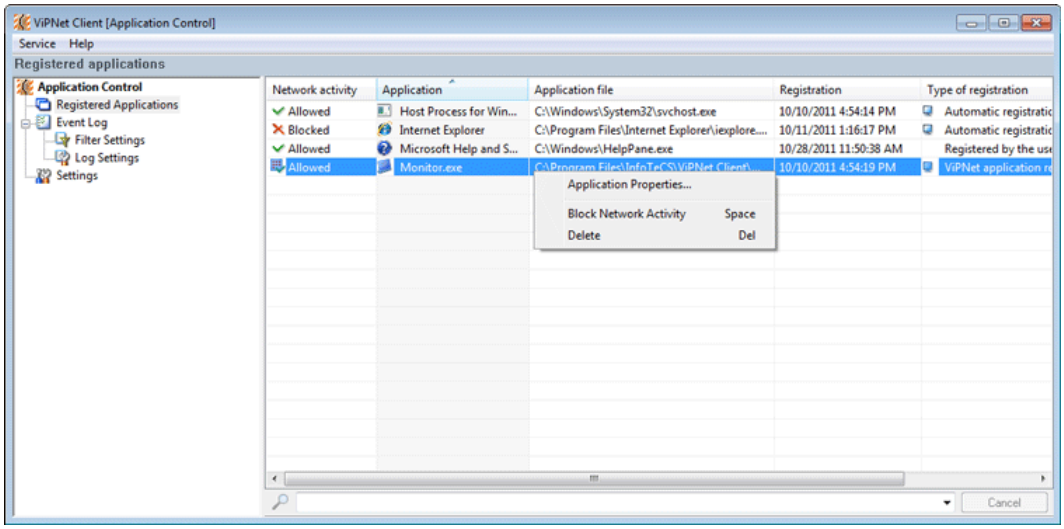


Figure 12: The list of registered applications

3 On the context menu, select the desired option:

- **Allow Network Activity**, if the application was blocked.
- **Block Network Activity**, if the application was allowed to connect to the network.
- **Delete**, for the request window to be displayed at the next application connection attempt. For more information, see Unregistering an Application (on page 36).

4 In the **Network activity** column of the table, the application status will be changed (if you have changed the application's network access rule) or the application will not be displayed in the table anymore (if you have chosen to remove it from the list of registered applications).

To configure a local application omitted in the list, you should register it manually (see Registering an Application Without a Request on page 24).

Unregistering an Application

Suppose you want to be prompted whether to allow or block network access for a certain application at its next network activity, although this application has already been registered. In this case, you should delete the application from the list of registered applications and set network access rules anew.

To unregister an application:

1. In the main window, in the navigation pane, select **Registered applications**.
2. In the **Registered applications** section, right-click the entry corresponding to the application you are going to unregister.
3. On the context menu, click **Delete**.

As a result, the removed application will be considered unregistered. At the next connection attempt of this application, Application Control will prompt you to set network access rules for it. You can re-register the application manually as well (see Registering an Application Without a Request on page 24).

Disabling Network Activity Tracking

Note: By default, Application Control is launched together with the ViPNet software it is part of and immediately starts tracking network activity of applications running on your computer.

If you disable the function of tracking network activity of applications, Application Control stops controlling the connections applications establish to the external network. On the one hand, it drastically decreases security of your computer, and malicious users may get access to your personal data. On the other hand, some software needs network access for correct functioning, and Application Control may prevent this application from establishing the required connection. Application Control is compatible with most programs requiring network access, however, in case of a third-party program failure, disabling network activity tracking may help to diagnose the problem cause.

Warning: To ensure your computer security, it is required that Application Control should be running. That is why you should re-enable network activity tracking as soon as the problem is solved. To enable the tracking, on the **Service** menu, click **Enable tracking**.

To disable network activity tracking, in the main window, on the **Service** menu, click **Disable tracking**. As a result, network activity of applications will not be tracked.

Changing a User

Different users can log onto Application Control. This means that several ViPNet users registered on the same host may work with Application Control, with a personal registered applications list and personal program options configuration each.

On one computer, several users may work with ViPNet Client or ViPNet Coordinator software (part of which Application Control is). The functionality of logging on as a different user allows each of the users to log onto the program using his or her own password, without closing the ViPNet software. To log on as another Application Control user:

1. In the main Application Control window, on the **Service** menu, click **Change user**.
2. In the logon window, in the **Password** box, type your password and click **OK**.

Note: If you log onto one ViPNet program as another user, this does not mean that you automatically change a user in all other ViPNet programs running on your host. For example, if you log onto ViPNet Monitor as another user, it does not mean that the user logged onto Application Control will change, and vice versa.

As a result, Application Control will be launched with the settings and the list of registered applications of another user.

Changing a User When You Work in a Terminal Session

A user can be changed in a terminal session, too. For example, if another user worked on a terminal server before you, and his or her program settings are configured in Application Control, you should log on with your password and work in your configuration. To do this:

1. In your user session, on the **Service** menu, select **Change User**.
2. Type your password and click **OK**.

As a result, in Application Control, your program settings will be used, and graphical interface will be refreshed in all user sessions running on this terminal server at the moment.

If, on a terminal server, several users try to change a user in Application Control simultaneously, only the first one to click **Change User** will be able to complete the operation.

Other users will be notified that another user is changing a user in Application Control and they should retry later.

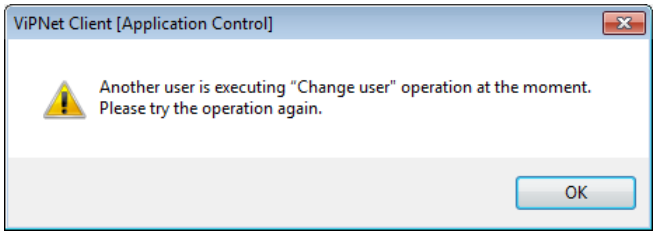

ViPNet Client [Application Control]
Another user is executing "Change user" operation at the moment.
Please try the operation again.
OK

Figure 13: Notification that a user change is happening in another user session at the moment

If, on a terminal server, one of the users is configuring Application Control, while another one is trying to log on as another user at the same time, the latter user will be notified that Application Control is being configured in another session and user change is not allowed at the moment. This user should retry later.

Logging onto Application Control as an Administrator

A ViPNet network administrator can log onto Application Control on any ViPNet host using the host administrator password or the "All Network" network group password. Then, the administrator can configure the options unavailable for a user because of insufficient permissions level.

To log on as an administrator:

1. In the main window, on the **Service** menu, click **Log in as Administrator**.
2. In the **Administrator Password** window, in the **Password** box, type the administrator password. Click **OK**.

As a result, all Application Control options will be available.

Logging onto Application Control As an Administrator When You Work in a Terminal Session

On a terminal server, you may need to log onto Application Control as an administrator to configure the options that are unavailable to you because of an insufficient permissions level.

If, on the terminal server, another user is logged on as an administrator at the moment, permissions levels in other user sessions will not change. However, the settings made by the administrator will be applied to Application Control in all user sessions.

Viewing Statistics and the Event Log

Viewing Statistics 43

Viewing the Event Log 44

Viewing Statistics

You can view information about registered applications either as:

- statistics, that is the total number of the applications registered and the number of applications allowed and blocked, or
- detailed information about the applications registered and their network status.

To view applications statistics, in the main window of Application Control, in the navigation pane, click **Application Control**.

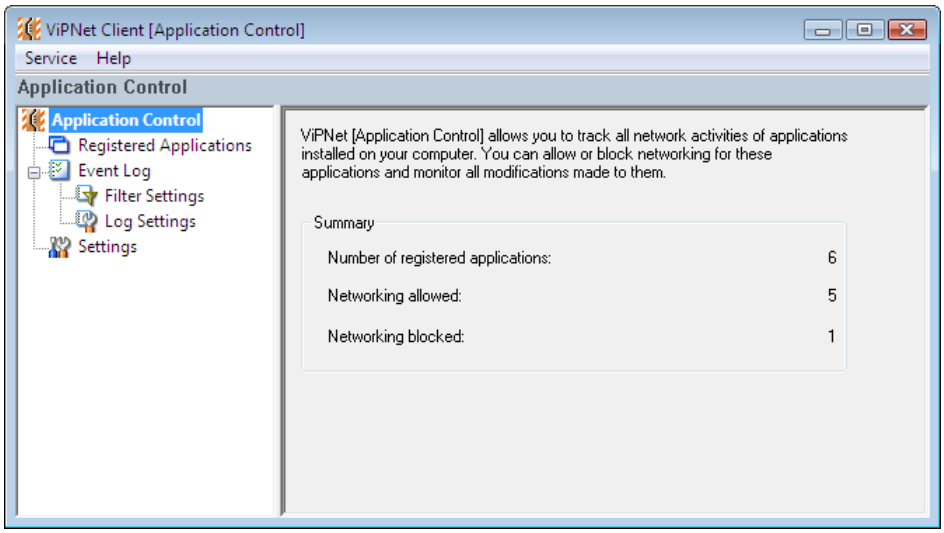

ViPNet Client [Application Control]
Service Help
Application Control
Application Control
Registered Applications
Event Log
Filter Settings
Log Settings
Settings
ViPNet [Application Control] allows you to track all network activities of applications installed on your computer. You can allow or block networking for these applications and monitor all modifications made to them.
Summary
Number of registered applications: 6
Networking allowed: 5
Networking blocked: 1

Figure 14: Viewing statistics for registered applications

In the **Application Control** section, you can view the following information:

- the total number of applications registered;
- the number of applications allowed to access the network;
- the number of applications that are not allowed to access the network.

Viewing the Event Log

The event log is displayed as a table containing information about status changes of registered applications. You can track what actions were applied to an application, and when. You can configure what information should be displayed in the log options (see Event Log Options on page 52) and in the options of the events filter (see Events Filter Options on page 54).

To view the event log:

1. In the main window of Application Control, in the navigation pane, select **Event Log**.
2. In the **Event Log** section, click **Refresh**.
3. As a result, a list of events will be displayed.

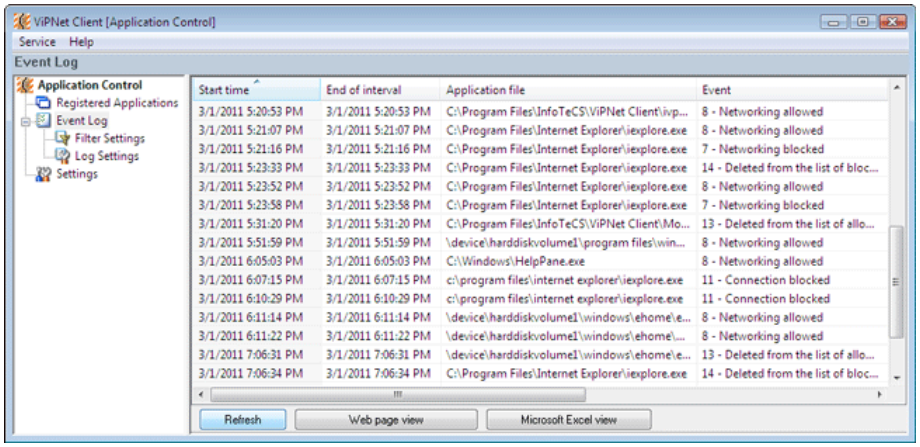


Figure 15: Properties of a registered application

You can view the event log in other programs:

- To view the event log in HTML, click **Web page view**.
- To view the event log as a Microsoft Excel table, click **Microsoft Excel view**.

When you are viewing the event log as a web page or a Microsoft Excel file, you can edit it, save and print for further usage.

There are 14 event types. They are described in the table below.

Table 4: The event types displayed in the Application Control event log

Event code	Event description
1	Blocked
2	Allowed
3	Network activity is blocked because the application was modified
4	Network activity is allowed after the application has been modified
5	Moved to the list of allowed applications by the user
6	Moved to the list of blocked applications by the user
7	Network activity blocked
8	Network activity allowed
9	Port is blocked to receive data
10	Port is opened to receive data
11	Connection blocked
12	Connection allowed
13	Deleted from the list of allowed applications by the user
14	Deleted from the list of blocked applications by the user

Configuring Application Control

Network Activity Tracking Options	47
Modifications Tracking Options	48
Processing Applications Network Access Requests in the Non-Interactive Mode	50
Event Log Options	52
Events Filter Options	54

Network Activity Tracking Options

You can set a network access rule for an application, that is, set an action to be applied to a tracked program at the program's connection attempt. To set a network access rule:

1 In the main window of Application Control, in the navigation pane, select **Settings**.

2 In the **Settings** section, under **Application control rules**, in the **At application network activity** list, select the desired rule (see Configuring Network Access for an Application on page 28).

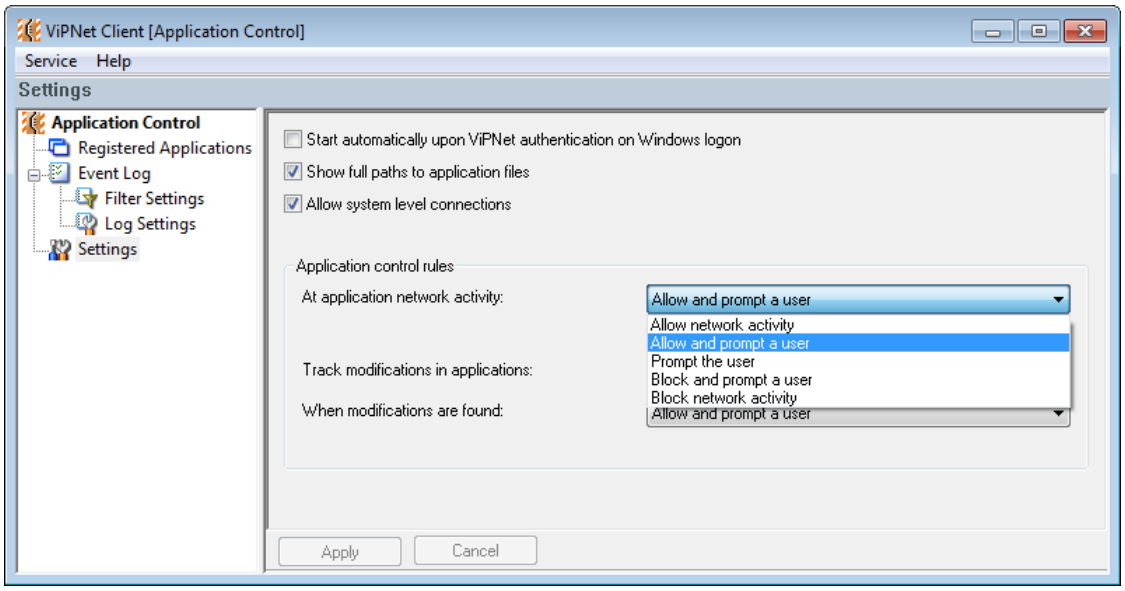


Figure 16: Configuring network activity tracking

3 By default, system-level connections are allowed. If necessary, for security purpose, to prevent a malicious user from establishing a connection to your computer on system behalf, clear the **Allow system level connections** check box.

Warning: Blocking of system-level connections may have negative impact. We recommend you to use this function only if you are an advanced Windows OS user.

4 Click **Apply**.

As a result, the chosen rules will be applied at the next connection attempt.

Modifications Tracking Options

After an application was registered in Application Control, it could be modified. On the one hand, the modification can be a result of normal application work, for example, of software update or adding new functions. On the other hand, malicious software could have modified the application registered, and you should block network access for the application then.

You can configure tracking of modifications in applications to define whether Application Control should track modifications, if yes, what modifications should be tracked, and what action should be applied to a tracked application if a modification is detected.

To configure modifications tracking:

1. In the main Application Control window, in the navigation pane, click **Settings**.
2. In the **Settings** section, under **Application control rules**, in the **Track modifications in applications** list, select one of the following options:
   - **By the application's file check sum**, in other words, by a certain value, verifying integrity and authenticity of the data transferred. As a result, if a modification of an application check sum is detected, you will be prompted to register the application anew.
   - **By the application's file size**. If a modification of the application executable file size is detected, you will be prompted to register the application anew.
   - **Do not track**. Modifications in applications will not influence the applications network access mode.

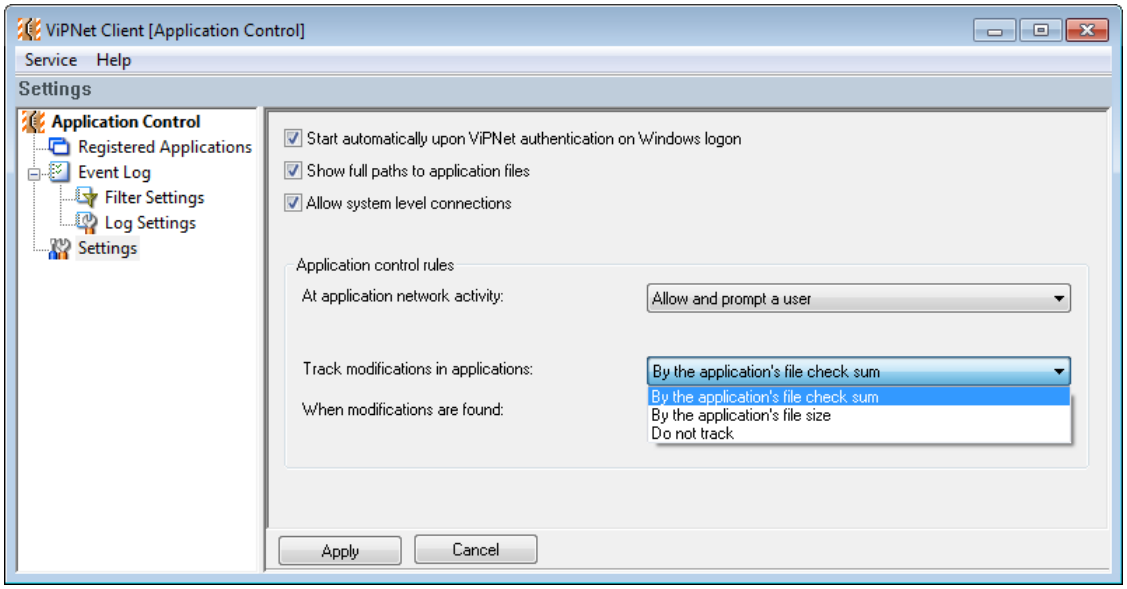


Figure 17: Configuring modifications tracking

3 Under **Application control rules**, in the **When modifications are found** list, select a network access rule. You can find the list of possible network access rules in **Configuring Network Access for an Application** (on page 28).

4 Click **Apply**.

As a result, at the next application network activity, the actions selected will be applied to the application.

Processing Applications Network Access Requests in the Non-Interactive Mode

The non-interactive mode of processing of applications network access requests ensures allowing or blocking applications network activity if one of the interactive network access rules (see Interactive network access rule on page 57) is set and if you can't choose ViPNet Application action in the request window at the moment. Requests are processed in the non-interactive mode in the following cases:

- your current user session has been blocked;
- Application Control is not running;
- at operating system startup, before you log onto the ViPNet software installed together with Application Control.

For example, you may need to allow applications network activity in the non-interactive mode at operating system services startup, when Application Control has already begun tracking applications network activity, but you have not logged onto the ViPNet software installed together with Application Control yet. The services should be allowed to access network at time to avoid problems with system startup.

If the **Allow and prompt a user** or **Block and prompt a user** network access rule has been set, in the non-interactive mode, network applications activity will be allowed or blocked according to it (as well as in the interactive mode), In the interactive mode, you will also be prompted to choose future Application Control actions for applications.

If the **Prompt the user** network access rule has been set, in the non-interactive mode, by default, applications network activity will be allowed. To block applications network activity at processing network access requests in the non-interactive mode:

1. In the navigation pane of the main Application Control window, click **Settings**.
2. In the view pane, under **Application control rules**, clear the **Allow network activity in noninteractive mode** check box(es).

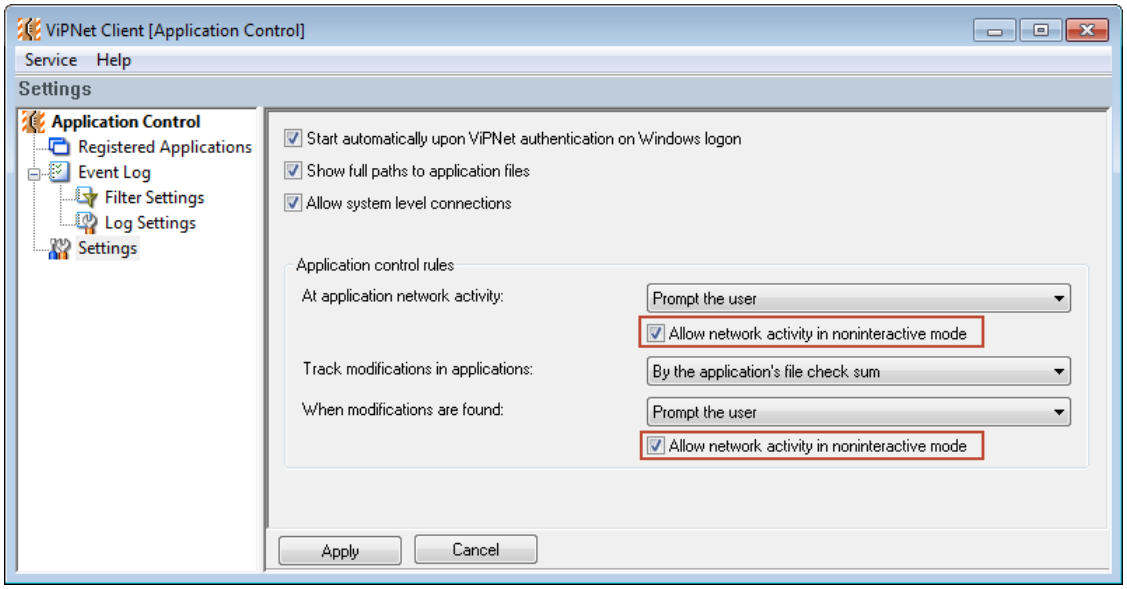


Figure 18: Configuring processing of network access requests in the non-intercative mode

3 Click **Apply**.

As a result, in the non-interactive mode, applications network activity will be blocked.

Event Log Options

You can configure the maximum file size of the event log (see Viewing the Event Log on page 44), the type of events (network activities) logged, log refresh options. To configure the event log:

1. In the navigation pane, expand **Event Log**.
2. Select **Log Settings**.
3. To define the maximum log size, in the corresponding box, type or select the required value (in megabytes). As soon as the log size reaches the specified value, all its entries are archived in the chronological order. If you set the parameter value to **0**, no limitations will be applied to the log size.

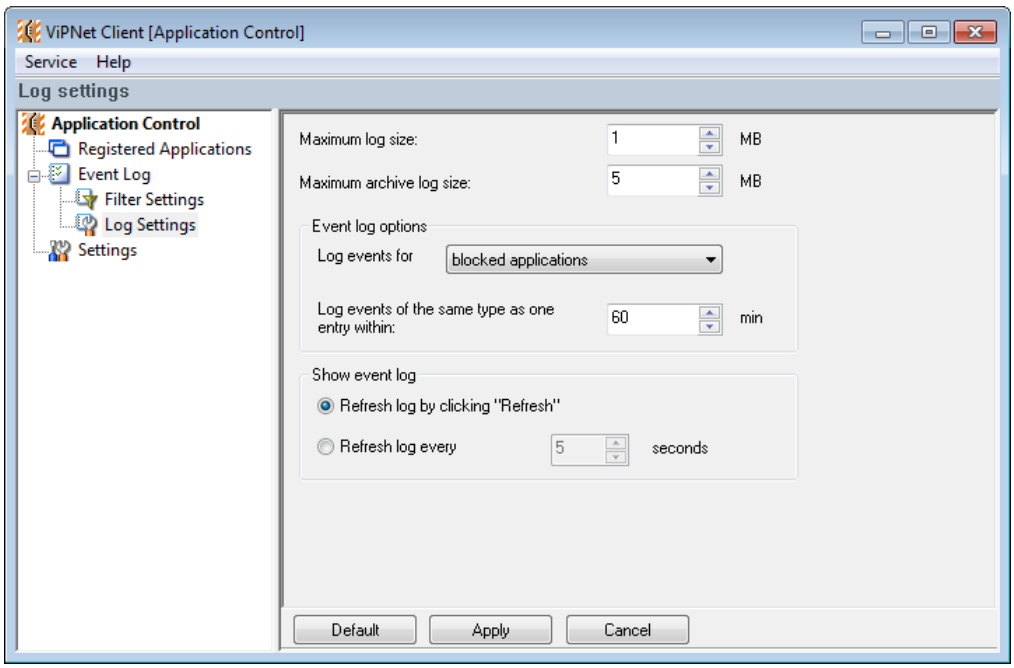


Figure 19: Configuring the event log

4. To define the maximum archive size, in the corresponding box, type or select the required value (in megabytes). As soon as the archive size reaches the specified value, the oldest entries are deleted. If you set the parameter value to **0**, no limitations will be applied to the log size.
5. Under E**vent registration**, in the **Log events for** list, select the type of applications (allowed, blocked, all). Events associated with the type selected will be logged.

Warning: All events associated with changes in the registered applications list (event code 3, 4, 5, 6, 7, 8, 13, 14) are always logged, regardless of the option chosen in the Register events list.

6 In the **Log events of the same type as one entry within** box, type or select the required value (in minutes). The default value is **60**. As a result, all events of the same type, in other words, all events with the same parameters, except for the exact time, will be logged in a single entry.

Note: To log each of the above-mentioned events in a separate entry, in the **Log events of the same type as one entry within** box, type or select **0**.

7 To configure log refreshing, under **Show event log**:

- to refresh the event log manually, select **Refresh log by clicking "Refresh"**;
- to refresh the event log automatically, select **Refresh log every** and specify the refresh interval (in seconds).

8 Click **Apply**.

As a result, the log and archive size, the type of registered events, and the log refresh options will be configured.

Events Filter Options

You can configure, how events will be displayed in the **Event Log** section, by using the events filter. Filtering events allows you to find certain events, for example, events associated with a certain application or IP address.

To configure the events filter:

1. In the main Application Control window, in the navigation pane, expand **Event Log**.
2. Select **Filter Settings**.
3. To specify the time interval within which the events will be displayed, under **Time interval**, select one of the options and specify the desired value.

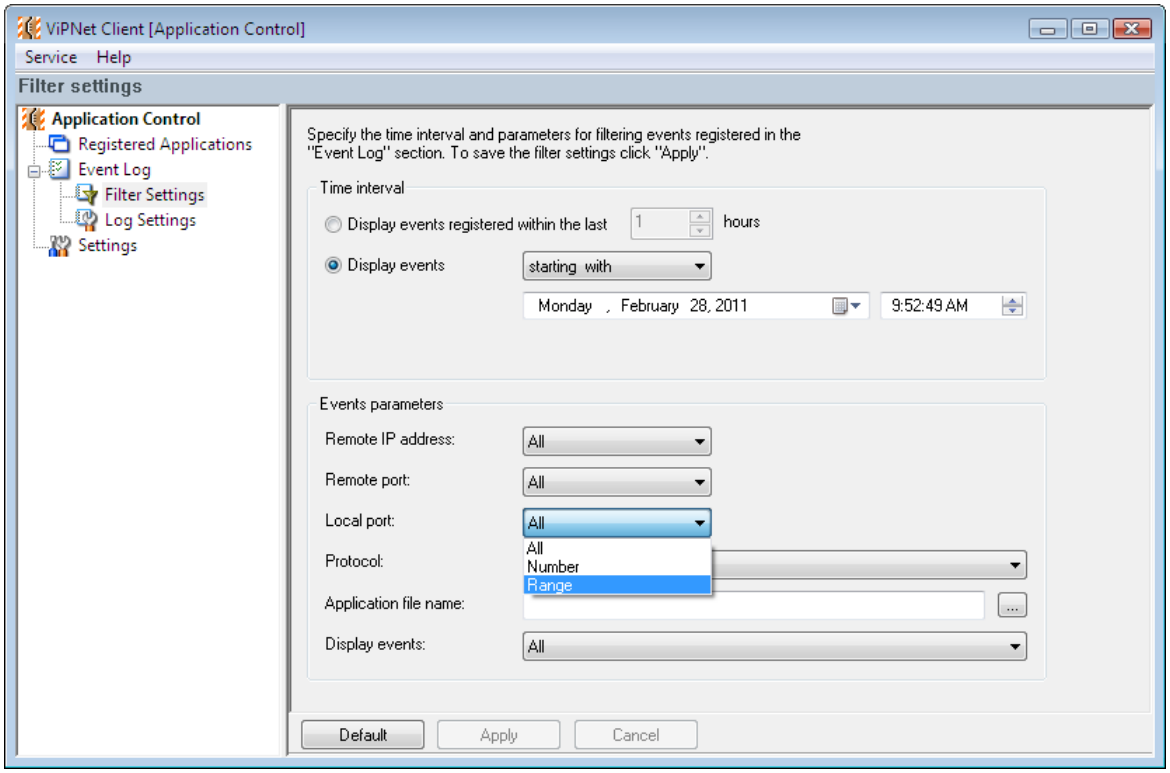


Figure 20: Filtering log events

4. To configure other event parameters, such as the remote IP address and port, local port, protocol, application file name, event type, under **Event parameters**, specify the desired values.
5. Click **Apply**.

For example, you need to view events associated with a torrent client uTorrent within a specified time interval. For example:

1. In the main window, in the navigation pane, expand **Event Log**.
2. Click **Filter Settings**.
3. Under **Time interval**, in the **Display events** list, select within and specify the required dates.
4. Under **Events parameters**:
   - In the **Protocol list**, select **TCP (Transmission control protocol)**.
   - In the **Application file name** box, specify `utorrent.exe`.
   - Make sure that, in the **Display events** list, it is selected **All**.

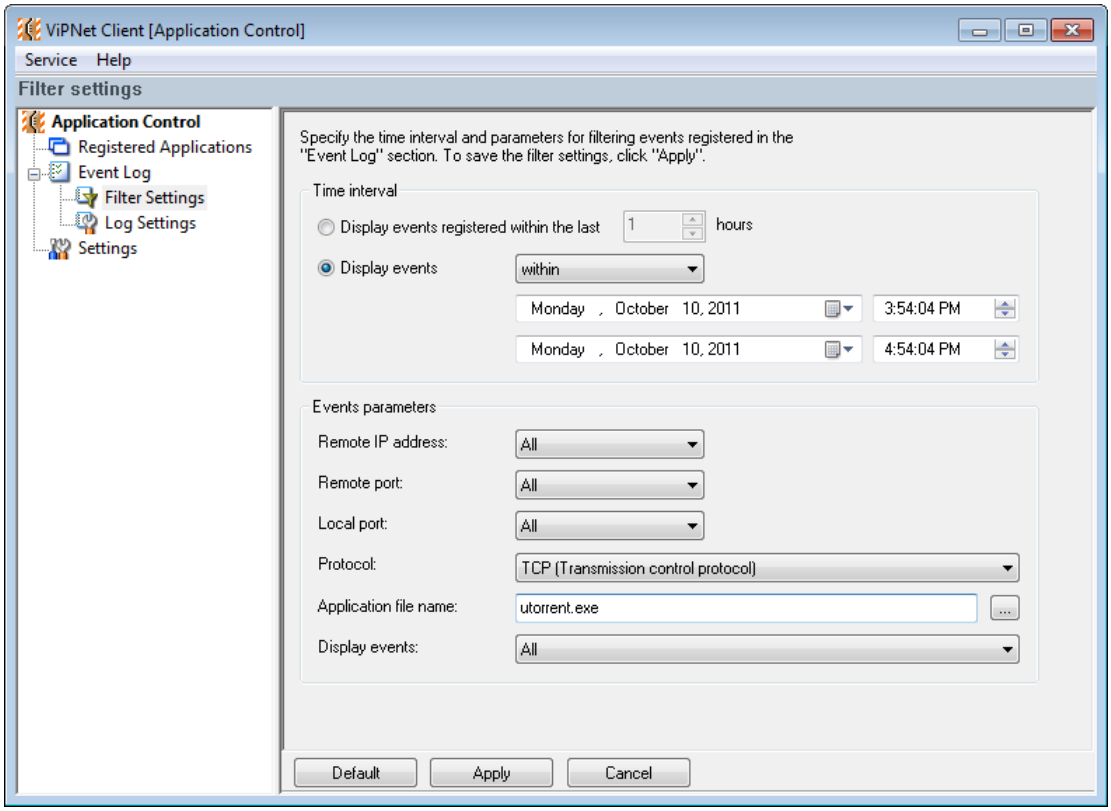


Figure 21: Configuring a filter to display torrent client uTorrent events

5. Click **Apply**.

As a result, in the **Event Log** section, only the events with the specified parameters will be displayed.

Glossary

I

Interactive network access rule

One of the network access rules applied in ViPNet Application Control. When you use an interactive network access rule, you define the way network activity requests from a certain application are processed. Interactive network access rules are:

- “Allow and prompt a user;”
- “Prompt the user;”
- “Block and prompt a user.”

L

License

A file allowing you to use certain ViPNet functionality. A ViPNet network license defines the maximum number of: coordinators in the network, clients registered on the coordinators, unprotected hosts tunneled by one coordinator (tunneled connections) and some other parameters.

See also: Client (ViPNet Client), Coordinator (ViPNet Coordinator), Tunneling, ViPNet network.

N

Non-interactive mode

A mode of processing application network activity requests, when Application Control automatically defines the action to apply.

U

User permissions

Rights defining whether ViPNet users can change their ViPNet software settings and to what extent.

The ViPNet network administrator defines user permissions for a ViPNet host in role properties.

See also: Role, ViPNet host (on page 58), ViPNet host administrator's password (on page 58), ViPNet Network Manager administrator, ViPNet Network Control Center administrator.

V

ViPNet host

A network node with installed ViPNet software registered in ViPNet Network Control Center or in ViPNet Network Manager.

See also: ViPNet Network Control Center, ViPNet Network Manager.

ViPNet host administrator's password

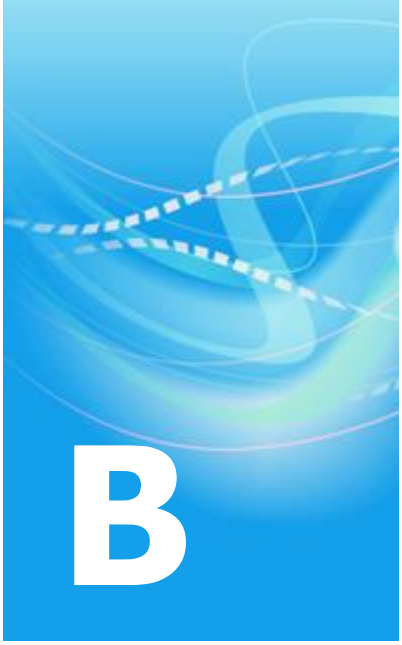
A password to enable the administrator mode on a ViPNet host. The administrator mode provides advanced options for the ViPNet program. A ViPNet host administrator’s password is created by the ViPNet network administrator in ViPNet Key and Certification Authority or ViPNet Network Manager.

See also: ViPNet host (on page 58), ViPNet Key and Certification Authority, ViPNet Network Manager.

ViPNet network administrator

A person responsible for configuring a ViPNet network, creating and updating keys and host links for ViPNet hosts, configuring partner network connections. This person has the permission to access ViPNet Network Control Center, ViPNet Key and Certification Authority, or ViPNet Network Manager.

See also: Keys and host links update, Partner network, Partner network connection, ViPNet Key and Certification Authority, ViPNet Network Manager, ViPNet Network Control Center.



Index

E
Event log • 45, 53, 55
Working in the non-interactive mode • 30, 51, 60

N
Network acces policy • 29, 30, 32, 36, 48
Allow and prompt a user • 20, 22, 30, 48
Allow network activity • 23, 29, 48
Block and prompt a user • 29, 32, 48
Block network activity • 23, 29, 48
Prompt the user • 29, 30, 48
Network activity • 8, 12
Network activity request • 20, 22, 23, 29

P
Permissions • 13, 60

R
Registration of an application • 12, 25, 44, 49
Deleting registered applications • 37
The list of registered applications • 36, 37

S
Starting and exiting the program • 27, 28
Administrator logon • 42
Changing user • 40
Disabling network activity control • 39

W
Working in a terminal session • 17, 33, 40, 42